|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  |  | | --- | --- | --- | --- | |  | | **PAYMENT CARD ACCEPTANCE POLICY** | | | Category: | VPOC | | | Approval: | *Sept 14th, 2015* | | | Responsibility: | *Associate Vice-Principal, Department of Financial Services* | | | Date: | *Date initially approved: Sept 14th, 2015*  *Date of last revision: TBD* | |  Definitions:A complete list of definitions can be found in the Payment Card Acceptance Procedures document.Purpose/Reason for Policy: The use of payment cards provides a convenient way for the University and authorized service providers to accept payment for goods and services. As a condition for the continued acceptance of payment cards, the University is contractually bound through its agreement with its payment card processing acquirers to be compliant with the requirements of PCI DSS.  The goal of PCI DSS is the protection of payment card data. PCI DSS is a comprehensive set of controls, processes, and other requirements designed to enhance payment card data security around the collection, storage, and handling of payment card information data.  All merchants are required to be compliant with PCI DSS for the continued acceptance of payment cards. Compliance with PCI DSS increases customer confidence for payment card transactions (e.g. donors); and provides a stronger internal control environment at the University with respect to the protection of sensitive information.  Non-compliance with PCI DSS exposes the University to risks including but not limited to:   * Potential loss of payment card acceptance privileges; * Liability for damages; * Damage to reputation; * Lost revenue and downtime for systems that are breached.  Scope of this Policy: This policy applies to any Queen’s department, faculty, or unit, employee, contractor and/or service provider operating on behalf of the University, who are involved in the acceptance, capturing, storage, transmittal, and/or processing of payment card data and/or who manages/oversees the completion of this work, on behalf of Queen’s, as part of their employment and/or contractual agreement with the University and/or applicable service providers. Policy Statement:  1. **Payment Card Industry Data Security Standard (PCI DSS)**   Any Queen’s department, faculty, or unit, employee, contractor or service provider operating on behalf of the University, or any University systems and/or networks that are involved with the acceptance, capturing, storage, transmittal, and/or processing of payment card data must be in compliance with the latest version of the PCI DSS to ensure the security of cardholder information, protect the University from reputational risk, financial and legal liability, and allow the University to maintain its ability to process payment card transactions.  1.1 Any Queen’s department, faculty, or unit, employee, contractor, or service provider operating on behalf of the University must demonstrate PCI compliance and receive approval from the PCI Coordinator before processing any payment card data.  1.2 All payment applications, solutions, or devices used for the acceptance, capture, storage, transmittal, and/or processing of payment card data must also be compliant with the latest version of the PCI DSS.  1.3 All third-party service providers used for the acceptance, capture, storage, transmittal, and/or processing of payment card data must demonstrate PCI compliance by providing a compliant AOC. There must be verbiage in the contract between the service provider and Queen’s to identify which party is responsible for managing PCI compliance.  Any failure to abide by this policy or the procedures contained in the Payment Card Acceptance Procedures may result in disciplinary action, including the temporary suspension or permanent revocation of payment card acceptance privileges.   1. **Establishment of Merchant Accounts**   Departments, faculties, and units may only accept payments through either a merchant account that has been established and approved by the Business Officer and PCI Coordinator, or through the [**One Time Events - Procedure for Accepting Credit Card Payments**](https://www.queensu.ca/financialservices/sites/finswww/files/uploaded_files/PCI/Merchant/One%20Time%20Events%20-%20Procedure%20for%20Accepting%20Payment%20Cards%20FINAL.pdf). The process to establish, modify, and close a merchant account can be found in the Payment Card Acceptance Procedures.  Merchant accounts must be established using the University’s approved acquirer(s). Departments, faculties, and units are prohibited from entering into other payment arrangements with non-approved service provider(s), including PayPal.   1. **Costs of Establishing a Merchant Account**   Any costs of establishing a merchant account for the purpose of accepting payment cards will be borne by the department, faculty, or unit establishing the account. These costs include, but are not limited to, the rental of POS terminals, the set-up and maintenance of a PCI terminal, installation of a cable for connectivity (if required), transaction fees, and costs associated with online e-commerce applications, payment applications, and service providers. In addition, merchants will be responsible for any costs associated with achieving and maintaining compliance with PCI DSS standards that occur outside of the core services (security scanning, auditing, and remediation work to ensure PCI compliance) offered by Financial Services and ITS. Merchants will also be responsible for costs associated with any security breaches as result of any non-compliance with the requirements of this policy and associated procedures.   1. **Exemption Requests**   Requests for exemptions to this policy must be approved by the PCI Coordinator, with authorization from the CPPSC where necessary. The process to submit an exemption is detailed in the Payment Card Acceptance Procedures.  Any merchant who receives an approved policy exemption is responsible for the administration associated with their merchant account. This includes ordering and installing equipment and managing user access. Equipment and user access for specialized payment applications must adhere to the PCI DSS requirements for user accounts.  Merchants who receive an approved policy exemption will be responsible for any additional costs and resources arising from the use and implementation of the exempted payment application and/or service provider. In addition, the Merchant will also be responsible for any costs related for ensuring that the payment application and/or service provider is compliant with all payment card compliance standards. Responsibilities:Merchants who interact with payment card data under the scope of this policy are responsible for adhering to the policy and procedural requirements for the acceptance, capture, transmission, storage and/or disposal of payment card data, and the [Queen’s Data Classification Scheme](http://www.queensu.ca/its/security/policies-procedures/standards/data-classification). Payment card data can be classified as confidential. For example: cardholder name, PAN, card verification value, EMV chip data, mag stripe data, and/or card expiry date (when combined with the PAN).Any Queen’s department, faculty, or unit, employee, contractor and/or service provider operating on behalf of the University, involved in the acceptance, capturing, storage, transmittal and/or processing of payment cards, and/or who manages/oversees the completion of this work, on behalf of Queen’s, as part of their employment and/or contractual agreement with the University and/or applicable service providers, are responsible for ensuring that they are compliant with this policy and associated procedures. Specific responsibilities are outlined in the Payment Card Acceptance Procedures.The PCI Coordinator will oversee the enforcement of this policy and associated procedures. The PCI Coordinator is responsible to approve, and facilitate additional approvals required due to the nature of the changes, all new merchant accounts and any changes requested to existing merchant accounts. Decisions to suspend or revoke a merchant account will be made by the CPPSC.The Associate Vice-Principal, Finance is responsible for the administration of this policy and associated procedures.  |  |  | | --- | --- | | Contact Officer | PCI Coordinator | | Amendment Date | Mar 2019 | | Date for Next Review | Mar 2024 | | Related Policies, Procedures and Guidelines | * [*Payment Card Acceptance Procedures*](https://www.queensu.ca/financialservices/sites/finswww/files/uploaded_files/PCI/PaymentCardAcceptanceProcedure.pdf) * [*Electronic Information Security Policy Framework*](https://www.queensu.ca/secretariat/policies/senate/electronic-information-security-policy-framework) * [*Electronic Information Security Policy*](https://www.queensu.ca/secretariat/policies/senate/electronic-information-security-policy-framework/electronic-information-security) * [*Network and Systems Security Policy*](https://www.queensu.ca/secretariat/policies/senate/electronic-information-security-policy-framework/network-and-systems-security) * [*Records Retention Schedules*](https://archives.queensu.ca/records-retention-schedules)  [Access to Information and Protection of Privacy Policy](https://www.queensu.ca/secretariat/policies/administration-and-operations/access-information-and-protection-privacy-policy)[Payment Card Industry Data Security Standard](https://www.pcisecuritystandards.org/) | | Policies Superseded by This Policy | None | |
|  | |